REPORT DOCUMENTATION PAGE

1. Report Security Classification: UNCLASSIFIED

2. Security Classification Authority:

3. Declassification/Downgrading Schedule:

4. Distribution/Availability of Report: DISTRIBUTION STATEMENT A: APPROVED FOR PUBLIC RELEASE; DISTRIBUTION IS UNLIMITED.

5. Name of Performing Organization:
JOINT MILITARY OPERATIONS DEPARTMENT

6. Office Symbol: C	**7. Address**: NAVAL WAR COLLEGE 686 CUSHING ROAD NEWPORT, RI 02841-1207

8. Title (Include Security Classification): (UNCLASSIFIED)

THE MOST LIKELY NEMESIS TO TIMELY, ACCURATE ELECTRONIC INFORMATION

9. Personal Authors:
MAJOR KAY L. SPANNUTH

10.Type of Report: FINAL	**11. Date of Report**: 4 FEBRUARY 2002

12.Page Count: 24 **12A Paper Advisor (if any): CAPTAIN ROBIN BABB**

13.Supplementary Notation: A paper submitted to the Faculty of the NWC in partial satisfaction of the requirements of the JMO Department. The contents of this paper reflect my own personal views and are not necessarily endorsed by the NWC or the Department of the Navy.

14. Ten key words that relate to your paper:
CYBERWAR, INTEROPERABILITY, SECURITY, NETWORKS, TRAINING, COMMERCIAL OFF-THE-SHELF, INFORMATION TECHNOLOGY, INTERNET, COMMUNICATIONS EQUIPMENT, ELECTRONIC INFORMATION

15.Abstract:

Fighting enemy cyber attacks--it sounds exciting and many people are ready volunteers to help defeat the external attacks; however, the Department of Defense needs everyone to focus on the relatively mundane, internal (non-enemy) issues. The internal issues are the most likely nemesis to timely, accurate electronic information gathering and management for the Commanders-in-Chief (CINCs).

While choosing a hard-to-crack password or developing a Continuity of Operations Plan or testing for interoperability may not sound thrilling similar actions can spell the difference in getting timely, accurate information to the CINCs. Coming to grips with the numerous internal issues and implementing solutions is not necessarily technical or highly expensive; however, it will require strong advocacy from the CINCs.

16.Distribution / Availability of Abstract:	**Unclassified** **X**	**Same As Rpt**	**DTIC Users**

17.Abstract Security Classification: UNCLASSIFIED

18.Name of Responsible Individual: CHAIRMAN, JOINT MILITARY OPERATIONS DEPARTMENT

19.Telephone: 841-6461	**20.Office Symbol:** **C**

Security Classification of This Page **Unclassified**

Naval War College
Newport, RI

THE MOST LIKELY NEMESIS TO TIMELY, ACCURATE ELECTRONIC INFORMATION

By

Kay L. Spannuth
Major, United States Air Force

A paper submitted to the faculty of the Naval War College in partial satisfaction of the requirements of the Department of Joint Military Operations.

The contents of this paper reflect my own personal views and are not necessarily endorsed by the Naval War College or the Department of the Navy.

Signature: ______________________

4 February 2002

____
Faculty Advisor
Robin Babb, Captain, U.S. Navy

Report Documentation Page

Report Date 04 Feb 2002	**Report Type** N/A	**Dates Covered (from... to)** -

Title and Subtitle The Most Likely Nemesis to Timely, Accurate Electronic Information	**Contract Number**
	Grant Number
	Program Element Number
Author(s)	**Project Number**
	Task Number
	Work Unit Number
Performing Organization Name(s) and Address(es) Joint Military Operations Department Naval War College 686 Cushing Road Newport, RI 02841-1207	**Performing Organization Report Number**
Sponsoring/Monitoring Agency Name(s) and Address(es)	**Sponsor/Monitor's Acronym(s)**
	Sponsor/Monitor's Report Number(s)

Distribution/Availability Statement
Approved for public release, distribution unlimited

Supplementary Notes

Abstract

Fighting enemy cyber attacks--it sounds exciting and many people are ready volunteers to help defeat the external attacks; however, the Department of Defense needs everyone to focus on the relatively mundane, internal (non-enemy) issues. The internal issues are the most likely nemesis to timely, accurate electronic information gathering and management for the Commanders-in-Chief (CINCs). While choosing a hard-to-crack password or developing a Continuity of Operations Plan or testing for interoperability may not sound thrilling, similar actions can spell the difference in getting timely, accurate information to the CINCs. Coming to grips with the numerous internal issues and implementing solutions is not necessarily technical or highly expensive; however, it will require strong advocacy from the CINCs.

Subject Terms

Report Classification unclassified	**Classification of this page** unclassified
Classification of Abstract unclassified	**Limitation of Abstract** UU

Number of Pages
26

ABSTRACT

Fighting enemy cyber attacks--it sounds exciting and many people are ready volunteers to help defeat the external attacks; however, the Department of Defense needs everyone to focus on the relatively mundane, internal (non-enemy) issues. The internal issues are the most likely nemesis to timely, accurate electronic information gathering and management for the Commanders-in-Chief (CINCs).

While choosing a hard-to-crack password or developing a Continuity of Operations Plan or testing for interoperability may not sound thrilling, similar actions can spell the difference in getting timely, accurate information to the CINCs. Coming to grips with the numerous internal issues and implementing solutions is not necessarily extremely technical or highly expensive; however, it will require strong advocacy from the CINCs.

CONTENTS

INTRODUCTION

Terrorism, including cyber attacks, is foremost in military minds as the year 2002 unfolds. While enemy cyber attacks on networks are a legitimate concern, this author's thesis is internal (non-enemy) issues are the most likely nemesis to timely, accurate electronic information gathering and management for the Commanders-in-Chief (CINCs).

The CINCs' vulnerability to receiving untimely or inaccurate information is high because of actions by their own users and systems administrators along with decisions made at Service and DOD levels. By concentrating their efforts on issues within their immediate control, CINCs can eliminate some actions which delay or corrupt information and significantly improve their odds of having timely, accurate information. Discussion of intelligence systems are beyond the scope of this paper; however, they have problems comparable to some covered here and should undergo similar analysis.

This paper focuses on three internal areas: problems caused by deliberate personnel actions/decisions, inadequate security, and lack of interoperability. These areas, not all inclusive, illustrate the magnitude of internal issues facing CINCs, even though the external issues seem to generate the more sensational commentary and subsequent concern. Coming to grips with the internal issues and implementing solutions is not necessarily extremely technical or highly expensive. It will, however, require strong advocacy from the CINCs.

Examples are used to illustrate current internal concerns, followed by a counter-argument from an opponent's point of view that external (enemy) attacks are the most likely threat to CINCs' information. Next, conclusions drawn from the internal and external problems are presented. Lastly, recommended actions for CINCs concerning items within their sphere of control or influence are provided.

DELIBERATE PERSONNEL ACTIONS/DECISIONS

First, let's look at problems caused by personnel actions, both non-malicious and malicious. While DOD ensures background checks are done before someone receives a security clearance for access to classified information, little training is currently required before that same person is allowed to have an account on a network. Training and guidance have not kept pace with the rapid proliferation of networks; therefore, people are doing things that significantly affect network integrity and the information accessible through that network. Also, existing guidance does not always get widely disseminated and/or people are not following it. Enforcement of accountability for actions is non-existent or inconsistent.

For example, both training and guidance are critical in password selection--a key pre-requisite to network usage. Despite DOD policy dictating minimum standards for passwords, some systems do not require specific criteria; therefore, users often select easy to crack passwords. According to Major General Dave Bryan, USA, Commander of Joint Task Force-Computer Network Operations (JTF-CNO), the most common password at DOD is "password."[1]

Additionally, some users have the same password on multiple systems, share passwords with co-workers, do not use password-protected screen savers, or record passwords either on paper in an easily accessible location or in a file on the network. Users want passwords that are easy to remember, the ability to utilize the same password for access to more than one system, and aid co-workers during absences; however, these sloppy practices play right into the hand of a malicious insider. While desiring to trust fellow workers, everyone must "address the sobering fact that a majority of threats to proprietary information today originate within the pool of authorized users."[2]

Other user-controllable items affecting information integrity are installing software or hardware without proper consent, introducing disks or files to the system from outside sources without running a virus scanner, and using non-tested applications. Also, users sometimes contribute to the magnitude of a computer problem by not having a backup of their files. Users and system administrators need to work together to determine who does the backups, when they are done, and where they are stored. Then, if there is a loss of information, the restoral time and re-creation time is minimized.

System administrators also take actions to make their job easier, but at the expense of security. As the General Accounting Office's (GAO) chief technologist, Keith Rhodes, said, "workers, disgruntled or not, leave open back doors and work around security measures for convenience."[3] Also, creating and managing access policies and keeping user access information current are labor-intensive, leaving network access prone to being too permissive or out-of-date.[4] Additionally, changes to the user's capabilities can be cumbersome, especially during a rapid deployment for a contingency.

Service and DOD level decision makers are charging full speed ahead directing implementation of network and web-based technology; however, the ripple effect of their actions is taxing both users and system administrators. Network operations are complex, but the biggest hurdles are not technical. As illustrated in the recent installation of a new Navy network on the USS NIMITZ (CVN-68), the insufficient support tail of training, documentation, and repair parts were key contributors to the determination the network "fails to adequately support mission requirements."[5]

Another example concerns the Theater Battle Management Core System (TBMCS). The combining of three older programs into this one system for air battle management, including producing the air tasking order, has advantages; however, as the program managers acknowledge, it is a complex system that can overwhelm untrained people.[6] The Marines, expressing concerns about training, initially declined to vote for TBMCS.[7]

The two examples above point out that leaders and program managers, while anxious to get new capabilities to the user, must consider the complete picture before installing systems. If people are not properly trained, it is almost inevitable they will input information incorrectly, be less efficient, or in some other way affect the timely transmission of information. Additionally, a distinct line between theater-level systems and other systems does not exist--the systems are sharing the same networks--so even non-theater systems processing finance or personnel data could negatively affect the CINCs' ability to get timely, accurate information.

If the user of that finance or personnel system generates a problem or a system outage occurs in one portion of the network, it can impact CINC's users in another part of the network. Some networks have tools to detect problems and automatically take action to correct the situation. This is normally an efficient method; however, it is based on priorities for the whole network and can trigger a cascading effect as lower priority users are disconnected in order to reconnect higher priority users. Not every user is a "high priority" user; therefore, some are going to be disconnected for an undetermined (based on the severity of the situation) time frame.

Disruptions in service highlight the need for a feasible, practiced Continuity of Operations Plan (COOP) for communications systems and facilities. Based on an analysis of systems and functions, a COOP establishes priorities and actions required when major emergencies occur. Having one and practicing it are critical to minimizing downtime, reducing confusion, and clarifying expectations. The attacks on the Pentagon pointed out some deficiencies within DOD and other government offices, including an ill-equipped secondary facility and difficulty in accounting for personnel.[8]

All the Services are increasing user access to networks--which is not necessarily all good news for the CINCs. The impact of the Services' quest for easy connectivity for their people via Army Knowledge Online (AKO), One Air Force ... One Network, and Navy Marine Corps Internet (NMCI) is hard to gauge. AKO alone expects 1.2 million users. This includes active-duty military, Army Reserve, National Guard, civilian, family members, and retired personnel.[9] While each of the Services expect these networks to provide benefits, CINCs should be leery of lapses in training, security and interoperability and their overall impact to the information CINCs need.

Traffic overload on networks is already an issue, especially in deployed locations, so it stands to reason that more people using networks will increase the problem. Two facets of saturation are occurring--the human ability to digest the information and the volume of information transiting the available equipment.

Brigadier General Robert M. Shea, USMC, Director for Command, Control, Communications and Computers for the Marine Corps, cites information overload problems as early as the Gulf War. He states intelligence reports came from various sources and up to 97 percent of the information in those reports was identical, with perhaps 3 percent useful to the Marines. "We got mesmerized by reading the same thing over and over again, and we missed that three percent."[10] Now, a decade later and with capacity to generate more information, warriors are still susceptible to not being able to digest all the information.

During a recent interview for Military Information Technology magazine, Lieutenant General John L. Woodward, Jr., USAF, Deputy Chief of Staff for Communications and Information at Headquarters U.S. Air Force, mentioned one of the greatest needs for managing information is software that can analyze information and then portray relevant information based on the human's need.[11] Without this assistance, the information may be available; however, it may not get to the CINCs in a timely manner.

General Shea also commented about the second facet--volume of information transiting the available equipment. He questioned the secret Internet protocol router network's (SIPRNET) ability to handle a sudden surge in traffic if the nonsecure (unclassified) Internet protocol router network (NIPRNET) is unavailable. He stated, "To me, the SIPRNET is the single point of failure that needs to be addressed. What's the backup to the SIPRNET? What is plan B? I haven't found the answer to that yet."[12]

General Shea brings up some legitimate concerns. Even if SIPRNET can handle the information, there are other problems. Physical accessibility is one hurdle. If NIPRNET users do not have SIPRNET accounts or do not have a SIPRNET terminal in their work area, there will be a delay until new accounts are created, increased security problems by sharing accounts, or delays due to insufficient number of terminals. Conversely, if the SIPRNET is unavailable, the biggest issue is how to accomplish the mission without sending classified information over the unclassified NIPRNET.

In the past decade, DOD made a conscious decision, for both economic and technology reasons, to start relying on commercial products. While sensible in some respects, commercial off-the-shelf (COTS) products should concern CINCs in other areas. Electronic equipment that was once built specifically for military conditions is replaced by equipment any individual can buy at a local electronics store. This newer equipment, often designed for a normal business office or home, does not necessarily perform reliably under the rugged handling and environmental conditions of numerous deployments.[13]

Fixing COTS products at a deployed location can generate concerns for commanders if a civilian from the business community needs to come on-site. Response time, transportation, security clearance, and personal protection all become issues. Is the person a combatant or non-combatant? Will the commanders have to expend resources to escort and protect the civilian? What impact will that have on sending timely information to the CINCs?

In an effort to reduce the forward footprint, some communication support is depending on reachback capability instead of in-theater equipment and personnel. This is a good idea in terms of personnel safety and support tail, but it can leave CINCs with less control over the information timeliness and accuracy. Instead of on-site databases and system administrators, the information and expertise may be several satellite hops and thousands of miles away.

If stateside support is furnished by contractor personnel, a key factor may be the terms of the contract. Hours of support, response time to fix problems, and who determines priority order of fixes are just a few things which can affect the CINCs' information. While a goal of outsourcing is efficiency, the CINCs can't afford to find out in the middle of a crisis it meant a reduction in services.

All issues mentioned in this section can have a negative impact on getting timely, accurate information to CINCs; however, all are controllable by DOD personnel, whether by the lowest ranking user or the highest ranking decision maker. The common thread is training, awareness of network impacts, and pre-planning for potential problems.

INADEQUATE SECURITY

The second area of focus is security. Many good steps resulted from the Clinton administration's policy, Presidential Decision Directive-63 (PDD-63), to improve protection of physical and cyber-based systems essential to the U.S. economy and government operations; however, much work remains for critical infrastructure protection. Issued in May 1998, PDD-63 tasked government agencies to participate in various groups and appoint specific points of contact; however, it based attempts to improve protection on coordination and cooperation, not regulation.[14]

PDD-63's annual progress report in January 2001 shows over 12 pages of DOD actions, illustrating many initiatives; however, many actions improving procedures or network enhancements appear individual to one organization and not necessarily applied over all the organizations.[15] A consolidated approach would reap greater benefits.

Richard Clarke, formerly the National Security Council's (NSC) Coordinator for Security, Infrastructure Protection and Counterterrorism, said the NSC did not want a czar for information technology (IT) nor did it want to create an agency responsible for overseeing security for all agencies' information.[16] President Bush issued an Executive Order which modified the previous PDD-63 approach. He created the "President's Critical Infrastructure Protection Board" and named Mr. Clarke as the Board Chair and Special Advisor to the President for Cyberspace Security. Again, the Board is a "coordinating" committee.[17] "Coordinating" offices, without "control" will continue to leave the government with a conglomeration of systems with various levels of security.

Even with increased emphasis on security, the CINCs cannot assume security is incorporated into the systems they use. Numerous government agencies, including DOD, got an "F" for IT security planning in 2001 from a congressional subcommittee. The evaluation, required by the Government Information Security Reform Act (GISRA), may have an affect on budgets. The Office of Management and Budget, using its control over purse strings, may use the GISRA data to stop funding projects that do not adequately address security.[18] Until this criteria is enforced in every system, the CINCs' information remains vulnerable.

Deeply entwined with many other issues, decisions are constantly made balancing security with functionality. As Michael J. Jacobs, Director of the Information Assurance Directorate at the National Security Agency (NSA), states, functionality and security are "not necessarily complementary" and "managers frequently must sacrifice functionality to achieve security."[19]

Rich Pethia, Director of the Computer Emergency Response Team which was established in 1988 to be the point of contact for the Internet community, believes the computer industry focuses its engineering for ease of use and not on ease of security administration. He further states there are not enough technical experts who really know how to set up and manage secure systems properly.[20] While CINCs want the easiest, fastest methods to process information, especially during contingencies, a delicate balance between functionality and security needs to be achieved.

Newer technologies like personal digital assistants and wireless local area networks (LANs) are attractive not only in daily activities, but also in deployed locations. Both present some security vulnerabilities which should leave CINCs suspicious of using them in large quantities until better security is developed and implemented. For example, virus checkers and intrusion detection systems used on wired LANs do not exist for wireless LANs.[21]

Sometimes enacting security measures has negative side affects. For instance, Defense Message System (DMS) users need a card (called Fortezza) to send messages. The cards are created on a specific computer and given to the user. If security policy regarding that computer is breached, then all the cards created on that computer are invalidated and the user has to get a new card. Normally locked out of DMS until that new card arrives, the user would be unable to send any messages. This can cause a significant mission impact depending on actions needed to fix the situation and on the number of cards that must be re-created.[22]

CINCs should be aware of that example as DOD is implementing another security enhancement via the Common Access Card (CAC). In addition to replacing the current armed forces identification card, the CAC has a computer chip on the card which allows the user to log on to the computer, encrypt e-mail, and digitally sign documents.[23] Circumstances similar to the Fortezza card could result.

System administrators are also hampered by the quality of the security products available to use. DOD and intelligence organizations are "increasingly frustrated over the tendency to bring commercial security products to market before they are fully evaluated and all glitches fixed."[24] Michael Jacobs goes a step further and states, "the commercial sector cannot provide sufficient security solutions for the NSA's constituency in government."[25]

LACK OF INTEROPERABILITY

The final area to examine is interoperability. Lieutenant General Joseph K. Kellogg Jr., USA, Director, Command, Control, Communications and Computer Systems (J-6), the

Joint Staff, stated the most important goal for J-6 today is interoperability. Problems occur because, as General Kellogg says, "under the current Title X authority, the services train, maintain, and equip their forces. They build the systems with service intent in mind, and then work the joint piece later in the process."[26] "Add-on" interoperability can result in modifications to the systems which affect functionality and/or security.

Since changes to computer programs and systems are constantly being made, interoperability will always be an issue. DOD Directive 4630.5 and DOD Instruction 4630.8 mandate joint and combined certification testing for systems in use by U.S. forces.[27] The primary facility to conduct the testing is the Defense Information Systems Agency's Joint Interoperability Test Command (JITC) at Fort Huachuca, Arizona. JITC is tracking down systems in use which have not been certified for interoperability.[28] Currently, CINCs cannot be assured all their systems are working together to provide them accurate information.

The leadership push towards commercial off-the-shelf (COTS) equipment is a concern in this area too. COTS products can meet established standards and still not be interoperable. Standards normally are not written specifically enough to ensure interoperability. One example is two computer programs displaying graphical pictures on a screen. One user marked a target and saved the information in one program. Another user tried to display the same target using a different program; however, it showed the target as another object.[29] A problem like that could lead to a friendly fire casualty or major political issue.

Another example pertains to the inventory of chemical and biological warfare personnel protection equipment. Currently, there are at least nine systems used to track the inventory of protective equipment and they are not interoperable with the Defense Logistics Agency (DLA) system. In fact, the systems use different data fields and some do not contain relevant information about lot numbers or expiration dates; therefore, there is no easy method to determine the availability of equipment.[30] It can take a manual, labor-intensive process to determine force protection status against chemical and biological warfare.

Magnifying the frustration of this issue are current development efforts. The Air Force and Marine Corps are developing new inventory systems; however, neither is interoperable with the other systems used by DOD. Even though the GAO recommended DLA standardize to one of those systems, DLA is working on another system that won't be ready until 2005.[31] At a minimum, resources are being wasted on duplicate efforts and there is still no guarantee the solution will be interoperable or that each service will use the same solution.

As General Kellogg says, "It is that services acquire, by law, for themselves, and joint thoughts only come into play late in the acquisition process. We should begin to build joint first and not leave it to the last."[32] CINCs are the optimal people to endorse this "jointness first" since they are the ones most affected if it doesn't happen.

Even more problems with interoperability occur when the United States must work with coalitions and alliances. Exchanging timely information is a big concern in defending the Republic of Korea because of equipment differences, security classifications, frequency allocation issues, and terrain. While some manual interfaces and work-arounds have been developed, they take precious time that may not be available in the event of a sudden attack.[33]

Working with North Atlantic Treaty Organization (NATO) countries produces similar interoperability problems, but on a larger scale. A.T. Cooper, executive coordinator at NATO Headquarters Consultation, Command and Control Staff, warns that the biggest interoperability problem is with land forces and it may take six years before nations fully meet interoperability standards.[34]

COUNTER-ARGUMENT

Opponents of this author's thesis will quickly argue external (enemy) issues are the most likely menace to timely, accurate electronic information getting to the CINCs.

Discounting the presentation of internal issues as scare tactics of many things that “could” or “may” happen, thesis opponents can point out external attacks “are” happening now; therefore, the CINCs should be more concerned about the enemy.

With a modest investment in electronic equipment, the enemy eliminates time, space, and force issues and can be on a more even playing field with the U.S. in cyberspace. An enemy no longer needs large forces or close proximity to the physical battlefield in order to dramatically impact U.S. forces. Since there are 3 to 3.5 million computers on the NIPRNET and 70 percent of that network’s traffic transits the Internet, DOD is quite vulnerable to external cyber attacks.[35]

Dealing with the constant computer attacks on Pentagon networks, the JTF-CNO was on an “at-war footing” even before September 11th. According to JTF-CNO statistics, unauthorized “events” (any access attempt by an unathorized user) against DOD computers is rapidly increasing. Rising from 5,844 in 1998 to 23,662 in 2000, the expected 2001 figure was over 40,000--and that estimate was prior to the September terrorism.[36]

One of the successful attacks was a big news story in summer 2001. Within a week, the Code Red Worm virus and variants infected over 200,000 Internet computers. While the objective appeared to be to create a log-jam on the Internet and not actually alter information on specific DOD databases, it caused numerous problems at DOD locations and degraded the NIPRNET connection with the Internet.[37]

Also, successful cyber attacks by politically motivated people are escalating regional tensions. One example is the Pakistan-India conflict. In 1999, pro-Pakistan groups had only 45 successful attacks on Indian web sites for the whole year. In contrast, there were 275 in the first 8 months of 2001. One pro-Pakistan group also defaced U.S. web sites belonging to the Department of Energy and the Air Force.[38] Another example is the Israeli-Palestinian cyber conflicts which have defaced 200 web sites since October 2000. There were targets in at least 19 countries aimed at a wide gamut of domains, including terrorist/extremist, commercial, technology, financial, media, health, and education sites.[39]

Activities like these by a group intent on causing damage, rather than just being an annoyance, could spell huge problems for CINCs. Not only would they have problems trying to communicate with DOD personnel, but also with other government departments and non-government agencies.

Other potential enemies are also positioning themselves for cyber attacks. One person who thinks the threat of cyber terrorism is very real is Yonah Alexander, a senior fellow at Potomac Institute for Policy Studies, an Arlington, Virginia think tank. One of his concerns is the Iraq Net, a series of over 100 Web sites located in domains throughout the world. He feels Saddam Hussein would not hesitate to use it to overwhelm the United States' critical cyber-based infrastructures.[40]

Based on these examples, opponents of the author's thesis view the external threats as the most likely menace to timely, accurate information gathering and management for the CINCs.

CONCLUSIONS

While a relatively small number of potential enemies have the expertise and access to penetrate and damage DOD systems, the sheer number of DOD users and the number of systems they can access present a greater potential for problems. The majority of issues mentioned in this paper were in the human factor realm, either among the people authorized access to systems or those people in positions to make decisions about those systems. That means many solutions are within the CINCs' sphere of control or influence.

Thinking the communications/computer people will dig into their technical toolbox and magically find the answer is unrealistic. While advanced technology can solve some of the issues, human decisions are the key factor. It's going to take the CINCs' personal involvement to bring about changes in deliberate personnel actions/decisions, inadequate security, and lack of interoperability.

The average person in DOD or involved in providing DOD products has good intentions, believes in technology, and has a desire to get new capabilities to warfighters. However, whether through lack of knowledge, desire for ease of use, competitiveness, lack of "big picture" thinking, or inattention to detail, people are doing things which jeopardize the speed and accuracy of the information they want to get to the CINCs.

While there are legitimate concerns about enemy attacks, the CINCs have more ability to improve the internal problems. Services can assist by thinking "joint" from the conception of a system. If the CINCs and Services concentrate their efforts on resolving the internal problems, then DOD can focus more resources on external issues.

Added protection against external attacks, however, will not solve the existing internal problems. The internal issues will still be the most likely nemesis to getting timely, accurate information to the CINCs if the CINCs do not personally endorse changes.

RECOMMENDATIONS

CINCs need to be the strongest advocates for correcting internal problems to ensure timely, accurate information. While the J6s will do most of the leg-work, everyone using or furnishing communications equipment or services must know the CINCs definitely endorse the efforts. Provided below is a checklist of items for CINCs to implement within their sphere of control or sphere of influence. While not exhaustive, the list includes key items relevant to curbing the internal problems.

Items Within the CINC's Sphere of Control

- Clearly state (via policy letters, staff meetings, etc.) the expected actions regarding passwords, new software, disk usage, etc.

- Ensure appropriate discipline/ramifications (counseling, reprimands, revoke access, re-training, etc.) accompany non-compliance.

- Emphasize J6 role in providing essential support to the warfighter requires proper coordination on all communications issues.

- Ensure appropriate training is conducted and support time for training.

- Ensure operation of communications equipment/systems meets mission needs regarding hours of support, backup of files, etc. while maintenance occurs without a negative impact to daily operations.

- Ensure adherence to JTF-CNO guidance concerning reporting problems and implementing fixes to known security problems.

- Ensure a viable Continuity of Operations Plan (COOP) is maintained and periodically tested.

- Work with DISA to determine which systems have not passed interoperability testing and schedule them for certification.

Items Within the CINC's Sphere of Influence

- Use the Integrated Priority List to highlight communications security issues.

- Ensure an appropriate support tail (training, spare parts, etc.) exists for all systems.

- Request notification of changes in services (hours of support, levels of service, scheduled maintenance outages, etc.) at supporting sites.

- Encourage maintenance of a viable COOP at supporting sites and assist in establishing appropriate testing times.

- Ensure new systems/major modifications undergo DISA's interoperability testing as mandated by DOD Directive 4630.5 and DOD Instruction 4630.8.

- Support a joint approval process before a system is developed/purchased.

If the CINCs implement these recommendations, they will be well on their way to ensuring they have the right information at the right time to plan and fight any war.

NOTES

[1] Robert J. Kaufman, III, <robert.kaufman@lackland.af.mil> "Defense Information and Electronics Report," [E-mail to Kay Spannuth <kdotspan@earthlink.net> 14 September 2001.

[2] Christian B. Sheehy, "Insider Cybercrime Finds No Place to Hide," SIGNAL, (February 2001): 57.

[3] Keith Rhodes, quoted in William Jackson, "Security Pros Warned of Enemy Within," Government Computer News, 19 (November 2001): 28.

[4] Moti Dolgin, quoted in William Jackson, "Security Pros Warned of Enemy Within," Government Computer News, 19 (November 2001): 28.

[5] William Jackson, "Carrier's Net Runs Aground," Government Computer News, 19 (November 2001): 10.

[6] William Miller, "C2's Giant Step Forward," Military Information Technology, (Volume 5, Issue 3): 36.

[7] Chuck Paone, "TBMCS is System of Record for Air Battle Command and Control," <*http://eschq.hansom.af.mil/esc-pa/news/2000/dec%202000/tbmcs.htm*> [2 December 2001]

[8] Dipka Bhambhani, "Crisis Proves a Need for Disaster Planning," Government Computer News, 24 (September 2001): 1,12.

[9] Peter M. Cuviello, John C. Deal, and Marjorie Walrath, "Key to Army Transformation," Military Information Technology, (Volume 5, Issue 10): 16.

[10] Henry S. Kenyon, "Marines Consolidate Systems Architecture," SIGNAL, (September 2000): 56.

[11] JoAnn Sperber, "Network Warrior," Military Information Technology, (Volume 5, Issue 10): 24.

[12] Kenyon, 58.

[13] Alan D. Campen, "COTS Is Only as Good as the Shelf," SIGNAL, (January 2001): 32.

[14] "Presidential Decision Directive/NSC-63." Presidential Decision Directives. 22 May 1998. <*http://fas.org/irp/offdocs/pdd/pdd-63.htm*> [17 December 2001]

[15] "Report of the President of the United States on the Status of Federal Critical

Infrastructure Protection Activities." Presidential Decision Directives. January 2001. <*http://fas.org/irp/offdocs/pdd/*> [17 December 2001]

[16] William Jackson, "Bush Making New Plans for Cybersecurity," Government Computer News, 17 (September 2001): 1, 12.

[17] President, Executive Order, "Critical Infrastructure Protection in the Information Age." <*http://www.ciao.gov/News/EOonCriticalInfrastructureProtection101601.html*> [26 January 2002].

[18] William Jackson, "Government Gets a Collective F for Its IT Security," Government Computer News, 19 (November 2001): 12.

[19] Robert K. Ackerman, "Technology Challenges Vex Security Agency," SIGNAL, (August 2001): 24.

[20] Robert K. Ackerman, "Computer Security Experts Warn of Growing System Vulnerabilities," SIGNAL, (August 2000): 18.

[21] Richard W. Walker, "Air Force Lab Struggles to Get a Handle on Wireless Security," Government Computer News, 10 (September 2001): 19.

[22] David Gruber, <david.gruber@pentagon.af.mil> "Network Topics: CAW Compromises," [E-mail to Kenneth Gaines <kenneth.gaines@afpc.randolph.af.mil] 26 November 2001.

[23] Colleen M. Hermmann, "Common Access Card (CAC) Security, and Privacy," CHIPS, (Summer 2001): 29.

[24] Anthony L. Kimery, "You've Got Infected Mail," Military Information Technology, (Volume 5, Issue 5): 9.

[25] Ackerman, "Technology Challenges Vex Security Agency," 24.

[26] JoAnn Sperber, "Interoperability Enforcer," Military Information Technology, (Volume 5, Issue 5): 18.

[27] "JITC Testing Policy," <*http://jitc.fhu.disa.mil/policy.htm*> [26 January 2002].

[28] Robert K. Ackerman, "Digitized Battlefield Elements Tested for Joint Environment," SIGNAL, (May 2000): 24.

[29] ibid.

[30] Dan Verton, "Lack of IT integration hurts chem/bio warfare defenses," Computerworld, 8 (October 2001) <*http://www.computerworld.com/cwi*> [8 December 2001].

[31] ibid.

[32] Sperber, “Interoperability Enforcer,”: 19.

[33] John Di Genio, “U.S. Forces in Korea Face Unique Challenges,” SIGNAL, (October 2001): 43-44.

[34] Robert K. Ackerman, “NATO Wrestles With Technology,” SIGNAL, (September 2001): 17.

[35] Clarence A. Robinson, Jr, “A Powerful Vision,” SIGNAL, (August 2001): 20.

[36] Kaufman, “Defense Information and Electronics Report.”

[37] Robert J. Kaufman, III, <robert.kaufman@lackland.af.mil> “Code Red Worm and Possible Chinese Connection” [E-mail to Kay Spannuth <kdotspan@earthlink.net> [19 November 2001].

[38] Michael A. Vatis, Cyber Attacks During the War on Terrorism: A Predictive Analysis. (Hanover, NH: Institute for Security Technology Studies at Dartmouth College, 22 September 2001), 4-5.

[39] Robert J. Kaufman, III, <robert.kaufman@lackland.af.mil> “Background: Israeli - Palestinian Cyber Conflict” [E-mail to Kay Spannuth <kdotspan@earthlink.net> [19 November 2001].

[40] Joshua Dean, “Nation Unprepared For Cyber War, Experts Say,” GovExe.com, 19 (December 2001) <*http://ebird.dtic.mil/Dec2001/e20011220nation.htm*> [21 December 2001].

BIBLIOGRAPHY

Ackerman, Robert K. “Computer Security Experts Warn of Growing System Vulnerabilities.” SIGNAL, (August 2000): 17-20.

________. “Digitized Battlefield Elements Tested for Joint Environment.” SIGNAL, (May 2000): 23-27.

________. “NATO Wrestles With Technology,” SIGNAL, (September 2001): 16-19.

________. “Technology Challenges Vex Security Agency.” SIGNAL, (August 2001): 21-24.

Bhambhani, Dipka. “Crisis Proves a Need for Disaster Planning.” Government Computer News, 24 (September 2001): 1,12.

Berry, Sharon. “One Plan, 140 Actions, 500 Days to Execute.” SIGNAL, (November 2001): 49-51.

Briganti, Steve. “To Be or Not to Be...That is the (Security) Question.” CHIPS, (Summer 2001): 11-14.

Campen, Alan D. “COTS Is Only as Good as the Shelf.” SIGNAL, (January 2001): 31-32.

Cuviello, Peter M. and Deal, John C. and Walrath, Marjorie. “Key to Army Transformation.” Military Information Technology, Volume 5, Issue 10: 12-16.

Dean, Joshua. “Nation Unprepared For Cyber War, Experts Say.” GovExe.com, 19 (December 2001) <*http://ebird.dtic.mil/Dec2001/e20011220nation.htm*> [21 December 2001].

“Department of Defense Directive 4630.5,” Department of Defense Directives. 11 January 2002. <*http://jtic.fhu.disa.mil/ciidocs.htm*> [26 January 2002]

Di Genio, John. “U.S. Forces in Korea Face Unique Challenges.” SIGNAL, (October 2001): 43-45.

Forno, Richard. “September 11th Does Not Mean Cyberwar is Coming,” <*http://www.infowar.com/mil_c4i/01/mil_c4i_091401b_j.shtml*> [25 November 2001]

Gruber, David. <david.gruber@pentagon.af.mil> “Network Topics: CAW Compromises.” [E-mail to Kenneth Gaines <kenneth.gaines@afpc.randolph.af.mil] 26 November 2001.

Hermmann, Colleen M. “Common Access Card (CAC) Security, and Privacy.” CHIPS, (Summer 2001): 29.

Jackson William. “Bush Making New Plans for Cybersecurity,” Government Computer

News,
17 (September 2001): 1, 12.

________. "Carrier's Net Runs Aground." Government Computer News, 19 (November 2001): 1,10-11.

________. "Government Gets a Collective F for its IT Security." Government Computer News, 19 (November 2001): 12.

________. "Security Pros Warned of Enemy Within." Government Computer News, 19 (November 2001): 28.

"JITC Testing Policy," <*http://jitc.fhu.disa.mil/policy.htm*> [26 January 2002]

Kaufman, Robert J. III. <robert.kaufman@lackland.af.mil> "Background: Israeli - Palestinian
Cyber Conflict." [E-mail to Kay Spannuth <kdotspan@earthlink.net> 19 November 2001.

________. "Code Red Worm and Possible Chinese Connection." [E-mail to Kay Spannuth <kdotspan@earthlink.net> 19 November 2001.

________. "Defense Information and Electronics Report." [E-mail to Kay Spannuth <kdotspan@earthlink.net> 14 September 2001.

________. "NIPC Daily Report." [E-mail to Kay Spannuth <kdotspan@earthlink.net> 19 November 2001.

Kenyon, Henry S. "Marines Consolidate Systems Architecture." SIGNAL, (September 2000): 56.

Kimery, Anthony L. "You've Got Infected Mail." Military Information Technology, Volume 5,
Issue 5: 6-9.

Lawlor, Maryann. "Pacific Command Builds Electronic Bridges." SIGNAL, (November 2000):
51-55.

Miller, William. "C2's Giant Step Forward." Military Information Technology, Volume 5, Issue 3,: 34,36.

Onley, Dawn S. "Air Force Debates Security Value of PDAs." Government Computer News, 17 (September 2001): 39.

Paone, Chuck. "TBMCS is System of Record for Air Battle Command and Control," 21 December 2000. <*http://eschq.hansom.af.mil/esc-pa/news/2000/dec%202000/tbmcs.htm*>

[2 December 2001].

"Presidential Decision Directive/NSC-63." Presidential Decision Directives. 22 May 1998. <*http://fas.org/irp/offdocs/pdd/pdd-63.htm*> [17 December 2001].

"Report of the President of the United States on the Status of Federal Critical Infrastructure Protection Activities." Presidential Decision Directives. January 2001. <*http://fas.org/irp/offdocs/pdd/*> [17 December 2001].

Robinson, Clarence A. Jr. "Physical Disaster Propels Cybersecurity Initiatives." SIGNAL, (November 2001): 17-20.

________. "A Powerful Vision." SIGNAL, (August 2001): 17-20.

Sheehy, Christian B. "Insider Cybercrime Finds No Place to Hide." SIGNAL, (February 2001):
57-60.

Sperber, JoAnn. "Interoperability Enforcer." Military Information Technology, (Volume 5, Issue 5): 17-20.

________. "Network Warrior." Military Information Technology, (Volume 5, Issue 10): 21-25.

U.S. Congress. House. Committee on Government Reform. Information Technology - Essential But Vulnerable: How Prepared Are We for Attacks?: Hearing before the Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations <*http://www.cert.org/congressional_testimony/Pethia_testimony_Sep26.html*> [26 January 2002].

U.S. President. Executive Order. "Critical Infrastructure Protection in the Information Age." <*http://www.ciao.gov/News/EOonCriticalInfrastructureProtection101601.html*> [26 January 2002].

Vatis, Michael A. Cyber Attacks During the War on Terrorism: A Predictive Analysis. Hanover, NH: Institute for Security Technology Studies at Dartmouth College, 22 September 2001.

Verton, Dan. "Lack of IT Integration Hurts Chem/bio Warfare Defenses." Computerworld, 8 (October 2001) <*http://www.computerworld.com/cwi*> [8 December 2001].

Walker, Richard W. "Air Force Lab Struggles to Get a Handle on Wireless Security." Government Computer News, 10 (September 2001): 19.